CSCE 557: Introduction to Cryptography

1. Course number and name: CSCE 557: Introduction to Cryptography. Cross-listed as MATH 587

2. Credit: 3-hrs; Contact: 3 lecture periods of 50 minutes or 2 periods of 75 minutes per week

3. Instructor: Stephen Fenner

4. Textbook: William Stallings, *Cryptography and Network Security: Principles and Practice*, 5th edition, Prentice Hall, Englewood Cliffs, NJ, 2011.

5. Specific course information

a.Catalog description: Design of secret codes for secure communication, including encryption and integrity verification: ciphers, cryptographic hashing, and public key cryptosystems such as RSA. Mathematical principles underlying encryption. Code-breaking techniques. Cryptographic protocols.

b.Prerequisites: CSCE 145, MATH 241, and either CSCE 355 or MATH 574

c.CSCE 5xx elective

6. Specific goals for the course

a.Specific outcomes of instruction are that students will be able to:

1.Know the principles of cryptology and of cryptanalysis of historical ciphers
2.Know and apply the theory and practice of modern cryptographic systems
3.Know and apply the theory and practice of protocols (that will include cryptography) for secure electronic communication
4.Be aware of the social, ethical, and political issues surrounding cryptography and its use in (especially electronic) communications

b.As an elective this course cannot be counted upon to contribute to the attainment of any student outcome.

7. Topics covered and approximate weight (14 weeks, 4 hours/week, 56 hours total)

1. Mathematical preliminaries (8 hours)
2. Security uses of cryptography (3 hours)
3. Cryptanalysis of classical ciphers (3 hours)
4. Information theory; perfect secrecy; one-time pads (3 hours)
5. Product cryptosystems and block ciphers (3 hours)
6. AES (Advanced Encryption Standard) – Rijndael (3 hours)
7. Public key encryption and RSA (6 hours)
8. Digital signatures (3 hours)

9. Authentication and key exchange (4 hours)
10. Advanced topics (3 hours)
11. Reviews and tests (3 hours)

Difference between Undergraduate and Graduate Work:
Graduate students must complete a major project in addition to the other assignments.

Syllabus Flexibility: High. The instructor chooses the textbook, programming language, and projects.

Modification and Approval History:

Initial description September 2002
Revised June 2005 by Duncan Buell to update text and clarify objectives and topics
Revised June 2011 by Stephen Fenner